

Patent Application
Docket No. 34648-435USPT
ERAL00005

WHAT IS CLAIMED IS:

1 1. A method of synchronizing encrypted data in an
2 Internet Protocol based network, comprising the steps of:
3 encrypting a data packet to be transmitted;
4 generating a sequence number associated with said
5 encrypted data packet; and

6 transmitting said encrypted data packet together with
7 said sequence number via an Internet Protocol based link.

1 2. The method according to claim 1, further comprising
2 receiving said encrypted data packet together with said
3 sequence number and decrypting said encrypted data packet
4 based on a value of said sequence number.

1 3. The method according to claim 2, further comprising
2 checking said decrypted data packet for errors and sending
3 an error message if errors are detected in a predetermined
4 number of data packets.

Patent Application
Docket No. 34648-435USPT
ERAL00005

1 4. The method according to claim 3, further comprising
2 initiating a data recovery procedure after reception of said
3 error message.

1 5. The method according to claim 4, further comprising
2 resetting said sequence number to an initial value after
3 initiating said data recovery procedure.

1 6. The method according to claim 5, further comprising
2 issuing a sequence number reset notification message after
3 resetting said sequence number.

1 7. The method according to claim 1, further comprising
2 setting a length of said sequence number based on an amount
3 of jitter in said Internet Protocol based link.

1 8. The method according to claim 7, further comprising
2 dynamically adjusting said length of said sequence number to
3 compensate for changes in said amount of jitter in said
4 Internet Protocol based link.

1 9. An apparatus for synchronizing encrypted data in
2 an Internet Protocol based network, comprising:
3 an encryption/decryption module configured to encrypt
4 a data packet to be transmitted;
5 a sequence number processor in said encryption/
6 decryption module configured to generate a sequence number
7 associated with said encrypted data packet; and
8 a transceiver module connected to said encryption/
9 decryption module configured to transmit said encrypted data
10 packet together with said sequence number via an Internet
11 Protocol based link.

1 10. The apparatus according to claim 9, wherein said
2 sequence number processor is further configured to extract
3 a sequence number from a received encrypted data packet.

1 11. The apparatus according to claim 10, wherein said
2 encryption/decryption module is further configured to decrypt
3 said encrypted data packet based on a value of said extracted
4 sequence number.

1 12. The apparatus according to claim 11, further
2 comprising an error detection module configured to check said
3 decrypted data packet for errors and to cause an error
4 message to sent if errors are detected in a predetermined
5 number of data packets.

1 13. The apparatus according to claim 12, wherein said
2 error detection module is further configured to initiate a
3 data recovery procedure upon detecting that errors have
4 occurred in said predetermined number of data packets.

1 14. The apparatus according to claim 13, wherein said
2 sequence number processor is further configured to reset said
3 sequence number to an initial value after initiation of said
4 data recovery procedure.

1 15. The apparatus according to claim 14, wherein said
2 sequence number processor is further configured to issue a
3 sequence number reset notification message after said
4 sequence number is reset.

1 16. The apparatus according to claim 9, wherein said
2 sequence number processor is further configured to set a
3 length of said sequence number based on an amount of jitter
4 in said Internet Protocol based link.

1 17. The apparatus according to claim 16, wherein said
2 sequence number processor is further configured to
3 dynamically adjust said length of said sequence number to
4 compensate for changes in said amount of jitter in said
5 Internet Protocol based link.

1 18. An apparatus for synchronizing encrypted data in
2 an Internet Protocol based network, comprising:
3 an encryption/decryption module configured to encrypt
4 a data packet to be transmitted;
5 a sequence number processor in said encryption/
6 decryption module configured to generate a sequence number
7 associated with said encrypted data packet;
8 a transceiver module connected to said encryption/
9 decryption module configured to transmit said encrypted data
10 packet together with said sequence number via an Internet

11 Protocol based link, wherein said sequence number processor
12 is further configured to extract a sequence number from a
13 received encrypted data packet, and said encryption/
14 decryption module is further configured to decrypt said
15 encrypted data packet based on a value of said extracted
16 sequence number; and

17 an error detection module configured to check said
18 decrypted data packet for errors and to cause an error
19 message to be sent if errors are detected in a predetermined
20 number of data packets, said error detection module being
21 further configured to initiate a data recovery procedure upon
22 detecting that errors have occurred in said predetermined
23 number of data packets, wherein said sequence number
24 processor is further configured to reset said sequence number
25 to an initial value after initiation of said data recovery
26 procedure and to issue a sequence number reset notification
27 message after said sequence number is reset.